Monahan, Torin, and David Murakami Wood. 2018. Intelligence and Security. In Surveillance Studies: A Reader, edited by T. Monahan and D. Murakami Wood. New York: Oxford University Press, 147-151.

SECTION 6

INTELLIGENCE AND SECURITY

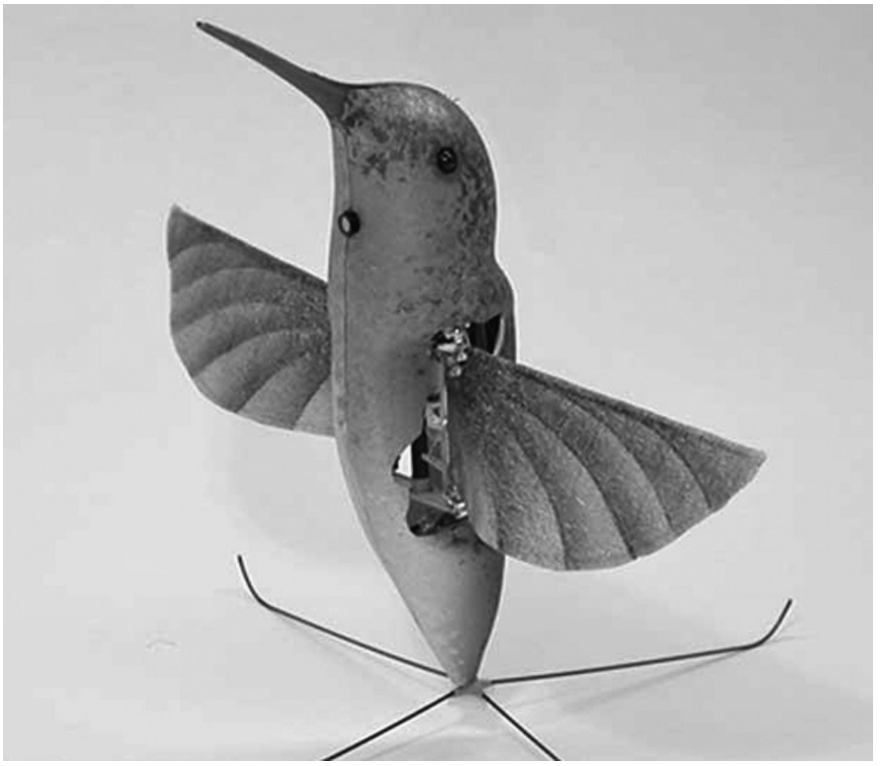
Edward Snowden rekindled interest in the murky world of state and military intelligence when he leaked US National Security Agency (NSA) documents in 2013. Two of the excerpts in this section concentrate on this agency: one from veteran journalist James Bamford's early 1980s account of the then little-known agency, and the other from journalist Glenn Greenwald, who was Snowden's initial contact. It is worth bearing in mind that however extensive the NSA's networks and programs, and however impressive its technologies, it remains just one powerful intelligence agency in a larger global network of allied national intelligence agencies.

Military interests intersect with and often motivate state intelligence operations. Although some of the writers who strongly influenced the direction of surveillance studies placed the development of surveillance within a broader context of militarism (e.g., Dandeker 1990; Giddens 1987), the military remained underemphasized until well after 9/11. In addition, studies of intelligence were largely carried out within a narrow, not very central subfield of international relations (IR) and security studies, and, reflecting the conservatism of IR more generally, were regarded with some skepticism if they deviated from official sources.

There are three interweaving streams of military surveillance development: warfare, occupation, and espionage. In the first stream, surveillance is concerned with knowing "the enemy" and the situation ("terrain"). Warfare overlaps with the history of many sociotechnical fields; for example, almost all technologies of flight have a military surveillance purpose or early adaptation (Adey 2010; Packer and Reeves 2013). Hot-air balloons were used to surveil troop deployments and defenses during nineteenth-century conflicts, including the US Civil War, and during the Cold War, supersonic and high-flying aircraft were used for military espionage, for example, America's U2 and SR-71 Blackbird planes. Now, new generations of drones or Unmanned Aerial Vehicles (UAVs) of all sizes operate from the edge of space right down to the battlefield (Parks and Kaplan 2017; Wall and Monahan 2011). The history of military camouflage, or art of evading surveillance, grew alongside these developments in verticality and optics (Shell 2012). The changing situation of conflict, in particular the renewed emphasis in the 1990s on fighting in cities (Military Operations in Urban Terrain—MOUT), has led to a military embrace of video surveillance and research and development of smaller, disguised sensors, many drawing from natural inspirations (so-called biomimetic devices), as well as of surveillance and combat robots. But, just as in Bentham's Panopticon where it was not only the inmates who were watched but

also the guards, in warfare, it is not just the "enemy" who is watched but also one's own soldiers. Military discipline was an early indicator of modern surveillance described in Foucault's (1977) *Discipline and Punish*. Perhaps the main reasons for such management are that soldiers are expensive but unreliable "assets": they are often reluctant to kill others; they suffer from fatigue; and they use illicit substances to stay awake, improve performance, or overcome combat boredom. The monitoring of troops has become increasingly technologized and intimate. For example, the US military research program "Objective Force Warrior" has attempted to develop real-time body sensors and automated medical systems—*somatic surveillance* (Monahan and Wall 2007)—incorporated into light-weight armored bodysuits for soldiers.

The second stream of military surveillance, as described in Alfred McCoy's *Policing America's Empire* (excerpted in Chapter 30), relates to the development of surveillance as a mode of counterinsurgency in imperial policing. McCoy's study is of US neo-imperialism in the Philippines and how the techniques devised there were not only developed into a whole strategic field of counter-insurgency that was widely used elsewhere, but were also "brought home" to the United States and drawn upon for internal political policing. Similar stories have been told of the United Kingdom, where techniques developed in the later period of the British Empire, such as fingerprinting in India, spread to other parts of the Empire, like Ireland, as well as to major English cities like London. These patterns can be witnessed in contemporary colonial situations too, as in the



AeroVironment Nano-Hummingbird, 2011, sponsored by US Defense Advanced Research Projects Agency (DARPA).

Israel-Palestine conflict described in the excerpt by Ahmad Sa'di, which presents a distillation of the bleeding edge of contemporary counterinsurgency surveillance techniques (see also Zureik, Lyon, and Abu-Laban 2011).

The final stream is the more conventional story of espionage. It was during the twentieth century that international espionage moved from being a rather intermittently used tool of government—very much subsidiary to diplomacy, as it had been, for example, since the formation of a small agency under Francis Walsingham during the reign of Elizabeth I of England in the sixteenth century—to being a key part of what former US president Eisenhower would call the "military-industrial complex." The foundation of early formal intelligence agencies took place largely during and after the First World War, with the Naval Intelligence division of the British Admiralty, then the most powerful military force in the world. The institutionalization and professionalization of state intelligence apparatuses accelerated in the decades after the war, with the forming of the US Central Intelligence Agency (CIA) in 1947 and the NSA in 1952, among others.

Although new technologies did not determine the direction of military and other surveillance practices, the synergy of perceived need, institutional commitment, postwar interdisciplinary experiments in cybernetics, and new technologies catalyzed a new formation of state intelligence. Technological developments in this environment were underpinned by new military-academic research fields—in particular, cybernetics and space science—and massively funded military research organizations, including the Advanced Research Projects Agency (ARPA—later, with the addition of "Defense," DARPA). The first consequential innovation was the computer, with its accelerated development occurring largely in response to sophisticated mechanical encryption deployed by German forces in the Second World War. The second, also an indirect product of that war, was the communications satellite, which US intelligence agencies began to operate from 1959 onward. And the third innovation was the growth of telecommunications technologies more generally. Each of these innovations would facilitate military espionage and surveillance more broadly.

These technological developments supported a massive global surveillance network. The United States solidified its dominance in this field by the end of World War II with the signing of agreements like the Britain-USA (BRUSA) agreement, relating to signals intelligence sharing, which was succeeded in the immediate postwar period by the UKUSA agreement. This agreement became the basis for what is now known as the "Five Eyes" network, with ex-British colonies Canada, Australia, and New Zealand added to the original partnership. As the excerpt reproduced here from Glenn Greenwald's book on the Snowden revelations shows, the spy network has greatly expanded to include many other willing and reluctant allies of the United States. Additionally, postwar Europe was saturated by a multiplicity of US counterinsurgency and intelligence operations, from the Gladio network of anti-Nazi agents, to cultural programs, which included the promotion of European political unification and anti-communist cultural initiatives. Similar networked intelligence efforts also occurred in the Soviet Union and the Warsaw Pact nations, as well as in several other countries, particularly France, which remained outside NATO and therefore developed an independent intelligence and satellite surveillance capability.

The potential for comprehensive forms of military surveillance was realized relatively early, with American military strategists in the Cold War period working toward what they conceived of as a "closed world" of total information control (Edwards 1996), which combined cybernetics and surveillance to

recreate the globe as a defensible, secure space. Along with the creation of multiple orbital satellite surveillance systems, this closed-world impulse also led in the late 1960s to the combination of computing and telecommunications into a secure, distributed packet-switching electronic communications system, ARPAnet, which would form the foundations for the Internet.

By the early 1990s, Manuel DeLanda (1991) could write without irony in his groundbreaking work, *War in the Age of Intelligent Machines*, of the emergence of a US military "panspectron," extending the logic of the Panopticon beyond the simply visible to all frequencies of the electromagnetic spectrum. At this time, in the immediate post–Cold War period, there were some briefly expressed hopes for a peace dividend and even a post-military society, but the so-called military-industrial complex rapidly diversified to cultivate civilian markets for surveillance and dataveillance products, as well as to maintain purely military production. This enabled the growth of an even larger, military-*security* complex, or a "neoconopticon" that emphasized private-sector involvement coupled with conservative political ideologies (Hayes 2009). Besides technological production, a variety of other indicators characterize this arena. These include, first, the transfer of discourse between civil and military fields: while the business world increasingly makes reference to "threat assessments," "information warfare," and "disruption," the military deploys business terminology, such as "core competencies" and "solutions," to describe its internal operations. This sharing of discourse is also part of a more profound shift in public-private partnerships among security organizations, seen for instance with the outsourcing of state intelligence work to private contractors. Roughly 70 percent of the US intelligence budget goes to private companies (Halchin 2015), and one should not forget that Snowden was an employee of one such company, Booz Allen Hamilton, when he accessed the NSA documents he would later leak. Another change is the increasing similarity of militaries and police forces. As the US military acts as a "global police," US military techniques and equipment have also infiltrated domestic police forces, as seen with military-like raids and the purchase and use of body armor, helmet-cams, and both lethal and "less lethal" weaponry. Military style intelligence programs have also "come home" in the post-9/11 period, with some examples being the growth of the Homeland Security field in the United States and the development of Fusion Centers and Domain Awareness Centers in cities across the country (Monahan 2011).

NOTE

It is worth outlining briefly the different types of security intelligence surveillance. The first is human intelligence (HUMINT), what one might call old-fashioned spying through contacts, informers, etc. This is traditionally what the US Central Intelligence Agency or Britain's MI6 do. With the growth of social media, a subdivision of HUMINT called open-source intelligence (OSINT) or social media intelligence (SOCMINT) has emerged. OSINT originally referred to conventional media monitoring, but now encompasses social media too. Signals intelligence (SIGINT) agencies deal with information that contains (either individually or in combination) communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). COMINT refers to information obtained for intelligence purposes from (foreign) communications interception and could thus be interpreted as including SOCMINT. Finally, another very important domain is imagery intelligence (IMINT) or photographic intelligence (PHOTINT).

REFERENCES

Adey, Peter. 2010. *Aerial Life: Spaces, Mobilities, Affects*. Malden, MA: Wiley-Blackwell.

Bauman, Zygmunt. 1995. *Life in Fragments: Essays in Postmodern Morality*. Oxford: Blackwell.

Dandeker, Christopher. 1990. *Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Cambridge, UK: Polity.

DeLanda, Manuel. 1991. *War in the Age of Intelligent Machines*. New York: Zone Books.

Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Vintage.

Giddens, Anthony. 1987. *The Nation-State and Violence: Volume 2 of A Contemporary Critique of Historical Materialism*. Berkeley: University of California Press.

Halchin, L. Elaine. 2015. The Intelligence Community and Its Use of Contractors: Congressional Oversight Issues. Congressional Research Service, August 18. Available from https://www.fas.org/sgp/crs/intel/R44157.pdf [accessed July 15, 2016].

Hayes, Ben. 2009. *Neoconopticon: The EU Security-Industrial Complex*. Statewatch and the Transnational Institute. Available from http://www.tni.org/sites/www.tni.org/files/download/neoconopticon_0.pdf [accessed May 17, 2013].

Monahan, Torin. 2011. The Future of Security? Surveillance Operations at Homeland Security Fusion Centers. *Social Justice* 37 (2–3):84–98.

Monahan, Torin, and Tyler Wall. 2007. Somatic Surveillance: Corporeal Control through Information Networks. *Surveillance & Society* 4 (3):154–73.

Packer, Jeremy, and Joshua Reeves. 2013. Romancing the Drone: Military Desire and Anthropophobia from SAGE to Swarm. *Canadian Journal of Communication* 38 (3):309–31.

Parks, Lisa, and Caren Kaplan, eds. 2017. *Life in the Age of Drone Warfare*. Durham, NC: Duke University Press.

Shell, Hanna Rose. 2012. *Hide and Seek: Camouflage, Photography, and the Media of Reconnaissance*. New York: Zone Books.

Wall, Tyler, and Torin Monahan. 2011. Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes. *Theoretical Criminology* 15 (3):239–54.

Zureik, Elia, David Lyon, and Yasmeen Abu-Laban, eds. 2011. *Surveillance and Control in Israel/Palestine: Population, Territory and Power*. New York: Routledge.